Information Security

Securing your data

It is important that all staff take due care to safeguard the security of LSTM research data as they are valuable assets that you will invest considerable time, effort and money in creating during the lifetime of the research project. Protecting your data from loss is therefore an important aspect of research data management and careful consideration should be taken in which environment you choose to store your data, what type of backup and retention systems to implement and levels of access that should be granted. This applies at all stages within the lifecycle of the project.

LSTM Information Classification Matrix

We have devised an information classification matrix to assist you in establishing a framework for classifying your data based on its level of sensitivity, value and criticality to LSTM as required by theCode of Practice for the Acceptable Use of Computer & IT Facilities at LSTM. Classification of information will aid in determining baseline security controls for the protection of data. For example, in helping to decide whether to transfer a file electronically via email or an encrypted email.

Recommendation for documentation

All LSTM staff have the facility to use One Drive for Business and we recommend that you always save important documents to this area of your hard drive. This area of your hard drive is automatically backed up and all staff have a minimum of 25GBs of file storage and this can be extended if required. Additionally, any files that you save in this area can be accessed remotely from any internet connected computer by going to http://portal.lstmed.ac.uk

Sharing documents internally

One Drive for Business is designed to store the files that are personal to you and not for files that are shared within a group. If you have files that you would like to share with colleagues internally then utilising a SharePoint site would be the better option. If you do not have a team site or if you want to learn about good examples of team-sites utilised at LSTM please contact Tom Cowlingtom.cowling@lstmed.ac.uk in LSTM IT Services.

The documents shared this way can also be synced to your hard drive so that when you're travelling without an internet connection you still have access to them please see user guide for more information.

Sharing documents externally

Whilst you can create external accounts for your SharePoint team-site, the syncing of files to the hard drive is not available for external accounts. External members would be required to login to the team-site to view documents.

There are other tools available for sharing documents / data depending on their data classification / sensitivity, such as Dropbox or Sugarsync. If you are in doubt about whether the system you are planning to use meets minimum security requirements then please contact the Director of IT Services (Eric Healing).

Other storage options

LSTM do not recommend the use of removal media for file storage. Please speak to LSTM IT Services before using this form of storage as it is likely that they can provide a more secure method of storage. It is also not advised that you store sensitive, personal data on a portable drive or on a laptop. Your attention is drawn to your responsibilities under the Data Protection Act, 1998 Further information and support on data protection can be found here and on the Information Commissioner's website.

Recommendation for patient identifiable data

Data that would allow the identification of individuals should not be stored on mobile device of any kind, this includes laptops. For sensitive data like this it should be kept in the country of origin and anonymised prior to transferring back to LSTM.

In the event of a non-anonymised data set being transferred to LSTM this should not be stored on the One Drive for business storage please contact LSTM IT Services for more information.

Anonymising your data

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to be able take place. A data set is not considered anonymised if you can still identify a participant from it. Typically you would remove names, initials, addresses and date of births and would then consider the data anonymised. However, the remaining information may be so specific to one individual which would then not be considered anonymised. Some further guidance is available in LSTM's Guide to anonymisation in clinical studies.